



Substitute for form 1449A/PTO <b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  (Use as many sheets as necessary)	<i>Complete if Known</i>	
	<b>Application Number</b>	10/781,311
	<b>Filing Date</b>	February 18, 2004
	<b>First Named Inventor</b>	Vincent Dupaquis
	<b>Group Art Unit</b>	2439
	<b>Examiner Name</b>	CHRISTIAN LAFORGIA
Sheet 1 of 1	Attorney Docket No: 2800.435US1	

US PATENT DOCUMENTS				
Examiner Initial *	USP Document Number	Publication Date	Name of Patentee or Applicant of cited Document	Filing Date If Appropriate
	US-2003/0079139A1	04/24/2003	Drexler, H., et al.	09/11/2002
	US-2003/0206629A1	11/06/2003	Eberle, Hans, et al.	03/11/2003
	US-2003/0208518A1	11/06/2003	Gura, Nils, et al.	03/11/2003
	US-2003/0212729A1	11/13/2003	Eberle, Hans, et al.	03/11/2003
	US-2004/0019622A1	01/29/2004	Elbe, Astrid, et al.	07/21/2003
	US-2004/0066934A1	04/08/2004	Chen, C.L	10/02/2002
	US-2006/0282491A1	12/14/2006	Joye, M.	06/17/2004
	US-5,185,711	02/09/1993	Hattori, Masayuki	12/06/1990
	US-6,049,815	04/11/2000	Lambert, Robert J., et al.	12/24/1997

FOREIGN PATENT DOCUMENTS				
Examiner Initials*	Foreign Document No	Publication Date	Name of Patentee or Applicant of cited Document	T <sup>1</sup>
	WO-06124160A2	11/23/2006	Dupaquis, Vincent, et al.	
	WO-2004111831A2	12/23/2004	Joye, M.	

OTHER DOCUMENTS – NON PATENT LITERATURE DOCUMENTS		
Examiner Initials*	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>1</sup>
	"European Application Serial No. 06749987.1 (Atty Ref 2800.489EP1), European Search Report mailed 05-28-2008", 14	
	"European Application Serial No. 06749987.1 (Atty Ref 2800.489EP1), EP Office Action mailed 10-01-2008", 3 pages	
	BAJARD, et al., "Arithmetic Operations in the Polynomial Modular Number System", RESEARCH REPORT LIRMM, no. 04030, XP002358296, (September 2004), 1-26	
	DE DINECHIN, B. D., "A Ultra Fast Euclidean Division Algorithm for Prime Memory Systems", ACM, (1991), 56-65	
	DHEM, JEAN-FRANCOIS, "Efficient Modular Reduction Algorithm in IFq[x] and Its Application to 'Left to Right' Modular Multiplication in IF2[x]", <u>Cryptographic Hardware and Embedded Systems - CHES 2003</u> , Volume 2779/2003, XP-002358295, Berlin, (2003), 203-213	

EXAMINER

DATE CONSIDERED

\* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant is to place a check mark here if English language Translation is attached